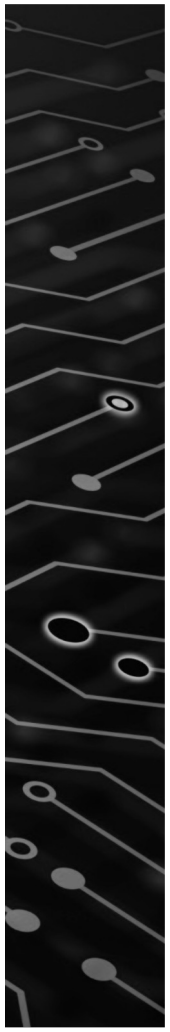
INSTITUTE FOR CYBER CIVICS

Conciencia sobre Ciberseguridad para Funcionarios Electorales y Trabajadores de Casilla

Material Informativo

v1.1 October 2024

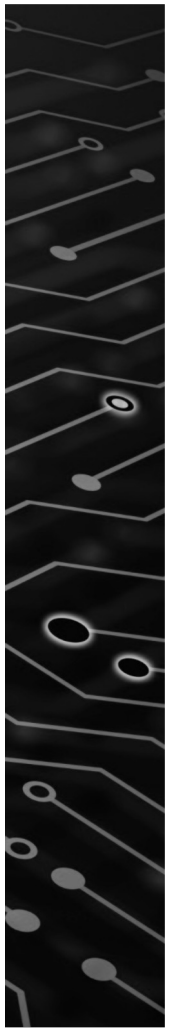
©2024 Institute for Cyber Civics, LLC. All Rights Reserved



Introducción y Glosario de Terminos

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Propósito de esta Guia



El propósito de este Manual es proporcionar a los Funcionarios Electorales y Trabajadores de Urnas una visión no partidista sobre cómo identificar posibles problemas de ciberseguridad durante la temporada de elecciones en los EE. UU. De acuerdo con la ley de cada estado, los Funcionarios Electorales desarrollarán y emitirán directrices oficiales y/o capacitación en las reglas y protocolos de su estado para los Trabajadores Electorales/Trabajadores de Urnas, así como para los roles de Observador Electoral/Observador de Urnas. Esta Guía está destinada con fines educativos específicamente para los funcionarios electorales, incluidos los trabajadores de urnas, es *voluntaria* y *complementaria* a cualquier orientación oficial de la Oficina de Elecciones del estado o del condado.

La intención del Instituto para la Ciber Cívica con esta Guía es educar al Funcionario Electoral y al Trabajador de Urnas sobre qué debe observar mientras desempeña sus deberes electorales. Aunque algunos de los temas son algo "técnicos", hemos proporcionado un Glosario en la Página 4 y también nos hemos enfocado en proporcionar "síntomas" observables de Problemas Potenciales, para que los Funcionarios Electorales puedan identificar más fácilmente un posible problema antes de que se agrave, incluso si dicho funcionario no es técnico.

Este documento no está destinado a ser profundamente técnico; para obtener especificaciones técnicas más detalladas, consulte otras publicaciones de nuestro Instituto o los enlaces disponibles en el sitio web de nuestro Instituto.

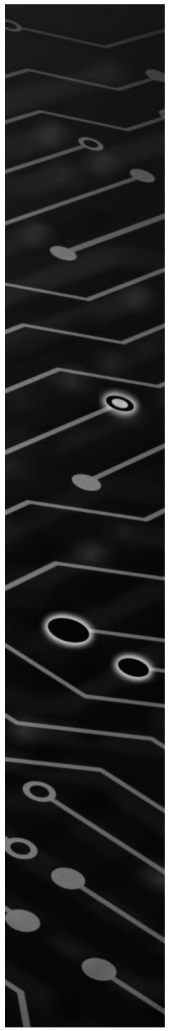
El dicho es cierto: ¡Si ves algo, di algo! En ciberseguridad, la velocidad es fundamental al identificar y abordar un posible problema. Ser vigilante, incluso con detalles o anomalías aparentemente sutiles, puede ayudarte a detectar un problema de ciberseguridad en sus primeras etapas. Como sabrás, es importante adherirse a las reglas y protocolos de tu estado. Con el propósito de estar preparado para posibles problemas cibernéticos:

Paso 1: Familiarízate con los escenarios de Problemas Cibernéticos Potenciales contenidos en esta Guía.

Paso 2: Durante la votación temprana y el Día de las Elecciones, prepárate para tomar notas detalladas sobre cualquier problema sospechoso que observes. Si está permitido, también te recomendamos capturar evidencia en foto/video.
Nuestro Instituto recomienda usar la aplicación ImageProof al capturar evidencia en foto y video. Descarga la aplicación (para iPhone y Android) en https://imageproof.io/. Las instrucciones están disponibles en el sitio web y en la aplicación. Nota: no se captura ninguna información de identificación personal ni datos del dispositivo cuando usas la aplicación ImageProof, ¡y las fotos y video que capturas en la aplicación son a prueba de manipulaciones!

Paso 3: Informa cualquier anormalidad de inmediato, de acuerdo con tus protocolos existentes. También te recomendamos contactar al Oficial de Seguridad de Información (CISO) de tu estado, ya que podrá proporcionar orientación técnica desde una perspectiva de seguridad.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved



Glossary of Terms

NO necesitas ser un experto en tecnología para identificar un posible problema de ciberseguridad. Familiarízate con el siguiente Glosario de Términos. Esto te ayudará a aprender sobre Posibles Problemas Cibernéticos a los que debes estar atento.

Acceso: Tu capacidad para llegar a algo, en el sentido físico, como acercarse a una computadora y tocarla, o en el sentido digital, como usar un teclado para escribir un ID digital y una contraseña para iniciar sesión en una computadora.

Código: Un conjunto de instrucciones escritas en un lenguaje que una computadora puede entender para realizar tareas específicas. Piensa en ello como una *receta* para una máquina:
• **Las instrucciones (código)** le dicen a la computadora qué hacer, paso a paso.
• **La computadora (chef)** sigue el código exactamente para obtener el resultado deseado, ya sea mostrar una página web, ejecutar un videojuego o calcular números.

Persona Interna: Una persona que tiene una identificación física o digital auténtica y válida con la cual puede acceder a sistemas o datos. Una "Persona Interna" también puede ser una amenaza si usa ese acceso con fines malintencionados.

Bitácoras: Son "diarios" que registran lo que está sucediendo en un sistema informático, una red o un software. Piénsalos como **diarios detallados** que registran cada evento importante: acciones, errores o cambios, para que las personas puedan revisar lo que sucedió. Imagina que es como **la torre de control de vuelos.** Los controladores escriben la llegada, salida y problemas de cada avión en un a bitácora. Si algo sale mal (como un vuelo retrasado), pueden mirar dicha bitácora para averiguar qué sucedió. Es lo mismo en los sistemas y el software, pero el sistema crea su propio registro que se puede inspeccionar cuando algo sale mal.

Red: Un grupo de dispositivos (como computadoras, teléfonos y servidores) conectados para que puedan comunicarse y compartir información entre ellos. ¡La red más grande es el **internet global**! Una red más pequeña puede ser como la que tienes en **casa** o en la **oficina**, donde tu teléfono se conecta a tu televisor inteligente o tu computadora portátil de trabajo se conecta a una impresora de trabajo. Una **red inalámbrica** (Wi-Fi) no requiere cables para que los dispositivos se conecten entre sí mediante señales de radio.

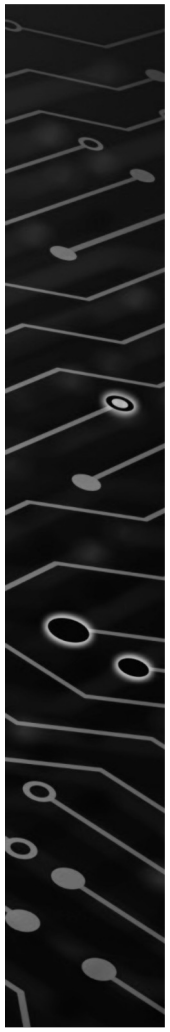
Una **red no segura** es aquella en la que cualquier persona con cualquier dispositivo puede conectarse a la red, sin necesidad de una contraseña o identificación, y acceder a internet. *Utilizar redes no seguras no es una práctica segura*.

Servidor: Una computadora potente que proporciona servicios, datos o recursos a otros dispositivos (como una computadora portátil, tableta o teléfono) a través de una red (como internet). Piensa en esto en términos de cómo funciona una cocina de restaurante:
• **La cocina (un servidor)** almacena ingredientes (datos) y recetas (software para usar los datos de ciertas maneras).
• **Los clientes (dispositivos)** hacen solicitudes a la cocina (el servidor), como pedir una pizza.
• **La cocina (el servidor)** prepara la comida utilizando ingredientes y recetas (datos y software) y envía el pedido correspondiente a la mesa (tu dispositivo).

Sala de servidores: Un espacio dedicado y controlado al que solo tienen acceso ciertas personas, que alberga servidores y otros equipos informáticos importantes necesarios para ejecutar sitios web, aplicaciones, bases de datos y redes. Es como el centro cerebral de las operaciones digitales.

Sistemas de votación o **Sistemas Electorales** o **Máquinas de Votación:** Cualquier tecnología, o cadena de tecnologías, a través de las cuales se llevan a cabo las elecciones. Estos sistemas y máquinas pueden incluir:
• Software de registro de votantes y los datos creados cuando un ciudadano se registra para votar.
• Estaciones de registro el día de la votación, e-books o computadoras portátiles, y el software que utilizan.
• Máquinas donde los votantes emiten sus votos y el software que tienen, así como los datos que producen (el voto).
• Máquinas de tabulación y el software que utilizan (para contar los votos).
• Servidores que soportan lo anterior y las redes a las que están conectados.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved



Problemas Cibernéticos Potenciales y Cómo Detectarlos

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema Potencial 1: Acceso No Autorizado a los Sistemas de Votación

¿Qué estoy buscando?

Mantente atento a **individuos inusuales o personas con credenciales sospechosas** que intenten acceder áreas donde se almacenan las máquinas de votación o que intenten acceder a los propios sistemas.

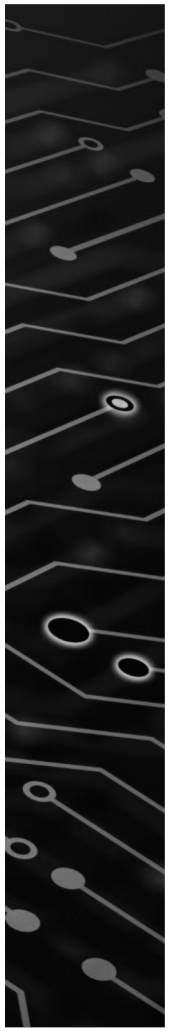
- Las credenciales adecuadas pueden incluir una placa oficial visible, con una foto adjunta que coincida con su apariencia
- En caso de tener duda, y si la persona está accediendo a áreas de almacenamiento o intentando acceder a las máquinas de votación, acércate de inmediato a la persona según tus protocolos oficiales.
- Vea también “Problema Potencial 2” – la bandera roja de actualizaciones de software o parches de sistemas en el Día de las Elecciones y “Problema Potencial 13 – Amenaza Interna”.

¿Por qué es esto importante?

Individuos no autorizados podrían cargar software malicioso o inyectar un código malicioso en un sistema electoral, lo que podría afectar la integridad de los resultados electorales.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema Potencial 2: Actualizaciones de Software el Día de las Elecciones



¿Qué estoy buscando?

Cualquier **intento de actualizar, parchear o dar servicio** a las máquinas de votación o sistemas electorales el Día de las Elecciones debería ser una señal de alerta.

- Las mejores prácticas en TI y Ciberseguridad establecen que los cambios en el software y el mantenimiento de las máquinas deben haberse completado mucho antes de que comience la votación, con pruebas completas realizadas por el personal de TI adecuado, y luego validadas por el(los) Funcionario(s) Electoral(es)
- Durante la votación, no debe haber mantenimiento de los sistemas de votación, parches al sistema o actualizaciones de software. Este período en el que no se deben hacer cambios se llama una 'Ventana de Congelación de Cambios'.

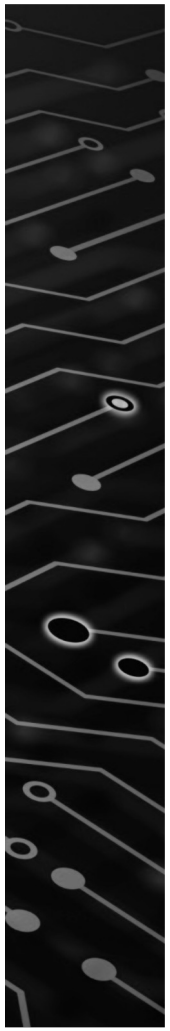
Independientemente de la justificación, razón o persona que realice el trabajo, no se debe permitir ningún intento de mantenimiento, parcheo o actualización del sistema el Día de las Elecciones, y se debe abordar de inmediato a la persona que intente realizar este trabajo según sus protocolos oficiales.

¿Por qué es esto importante?

Las actualizaciones del sistema o parches de software implementados mientras los sistemas electorales están en uso para la votación podrían interferir con la integridad de los datos de votación ya recopilados y/o podrían inyectar código malicioso en el software del sistema, lo que podría interferir con la integridad de los resultados electorales.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema Potencial 3: Dispositivos Externos Conectados a los Sistemas Electorales



¿Qué estoy buscando?

Esté atento a cualquier **manipulación física de las máquinas**. Las máquinas de votación deben tener sellos sobre cualquier puerto abierto (para que no se pueda insertar una unidad USB o cable) y, potencialmente, sobre las uniones de la propia máquina."

- Sospeche de cualquier unidad USB externa, tarjeta de memoria u otros dispositivos conectados a las máquinas de votación o sistemas electorales
- Esté alerta ante cualquier sello roto o un sello que parezca haber sido manipulado (por ejemplo, un borde levantado o una serración en él)
- Realice inspecciones visuales regulares y periódicas de los sistemas de votación, para asegurarse de que todos los sellos permanezcan intactos y sin manipulación, y que no haya dispositivos ni cables conectados a los sistemas de votación.

¿Por qué es esto importante?

Dispositivos insertables (como una unidad flash) podrían usarse para introducir software malicioso (malware) en el sistema electoral, lo que podría extraer o manipular datos sensibles de votación.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema Potencial 4: Comportamiento Inexplicado de la Máquina

¿Qué estoy buscando?

Preste atención a cualquier mal funcionamiento o comportamiento inusual de las máquinas de votación o estaciones de registro de votantes. El mal funcionamiento podría verse como:

- Retrasos en el procesamiento del sistema
- Reinicios automáticos
- Requerimiento frecuente de reinicios
- Congelamiento de la pantalla (BSOD o 'pantalla azul de la muerte')

Cualquiera de estos problemas podría manifestarse en *un solo* sistema, podría parecer que *múltiples* máquinas experimentan fallas simultáneamente, o podría aparecer como una falla en toda la infraestructura de votación de extremo a extremo. Informe cualquier problema de este tipo de inmediato: la rapidez es de suma importancia.

¿Por qué es esto importante?

Cualquiera de los comportamientos inexplicados de las máquinas mencionados anteriormente podría ser un indicio de fallas de hardware, bloqueos de software, infecciones de malware o intentos de hackeo del Sistema, cualquiera de los cuales puede interrumpir o interferir con las elecciones y/o socavar la integridad de las elecciones."

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema Potencial 5: Capacidades Inalámbricas No Aprobadas y Redes Inseguras

¿Qué estoy buscando?

Dependiendo de su estado, **puede estar prohibido que las máquinas de votación** tengan activadas las capacidades inalámbricas. En ciertas jurisdicciones, *una parte o toda* la infraestructura electoral **puede tener permitido** conectarse a una red segura. Conozca las reglas de su estado/condado.

En intervalos diferentes durante el día, inspeccione la configuración de *cada* sistema para lo siguiente:

- Si su estado *no* permite la conectividad, verifique que cada máquina NO esté conectada a NINGUNA red y que la capacidad inalámbrica esté desactivada
- Si su estado *si* permite la conectividad, verifique que los sistemas estén conectados ÚNICAMENTE a la red segura aprobada.

Una palabra sobre 'redes seguras':

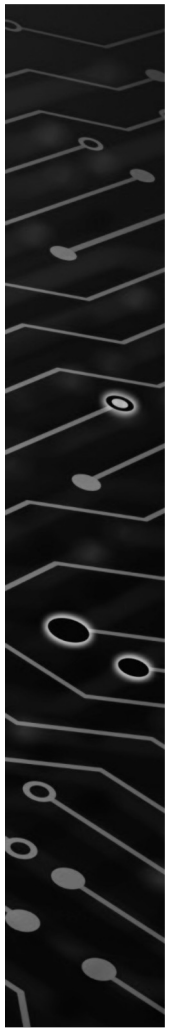
- La votación se realiza en lugares públicos que a menudo tienen una red inalámbrica de uso prolongado y ampliamente utilizada. Solo porque se informe que esta red es segura, puede que tenga la contraseña publicada para que el público la vea, o puede ser una contraseña compartida por empleados diarios que no se ha cambiado en años; esta no es una red segura.
- Asegúrese de que cualquier red utilizada por los sistemas de votación tenga una contraseña compleja establecida de nuevo para el Día de las Elecciones y que la red sea utilizada ÚNICAMENTE por los sistemas de votación y no para el uso general de los empleados o el público de esa instalación (por ejemplo, una biblioteca).

¿Por qué es esto importante?

Las máquinas que se conectan a una red cuando no deberían poder hacerlo en absoluto, o que se conectan a una red antigua o no aprobada, pueden crear una oportunidad para que un actor malintencionado obtenga acceso a los sistemas electorales o a los propios datos de votación.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema Potencial 6: Máquinas de Votación, Equipos o Cables sin Seguridad o sin Supervisión



¿Qué estoy buscando?

Las máquinas de votación y los sistemas electrónicos deben estar debidamente asegurados, y no debe haber máquinas desatendidas o sin supervisión, ni sistemas que no estén debidamente bloqueados o guardados bajo llave.

Buenas prácticas de ciberseguridad incluyen:

- Las salas de servidores, cables de red y conexiones utilizadas para el proceso electoral, así como las máquinas de votación no utilizadas, deben estar debidamente aseguradas en una sala que esté monitoreada en todo momento (por ejemplo, mediante una cámara de CCTV)
- Todo acceso a las salas de equipos electorales debe ser meticulosamente documentado (registro de entrada y salida)
- Todas las máquinas de votación y sistemas de registro en uso el día de las elecciones deben estar visibles para los funcionarios electorales. Ningún sistema en uso debe estar fuera de la vista (por ejemplo, debajo de un escritorio)
- Cualquier computadora portátil o sistema de registro electrónico utilizado en el proceso de votación debe tener la pantalla bloqueada cuando el usuario autorizado no esté frente a ella
- Cada pantalla debe requerir una identidad digital única y una contraseña para desbloquearse. Si esto no es posible, asegúrese de que cualquier identidad y/o contraseña compartida no sea visible para el público.

¿Por qué es esto importante?

Los dispositivos desatendidos pueden ser manipulados y potencialmente utilizados para acceder y alterar la infraestructura electoral y/o los datos de votación. Las credenciales de inicio de sesión compartidas son fácilmente manipulables por actores malintencionados. Las credenciales compartidas en varias máquinas pueden dificultar la captura de detalles necesarios para las investigaciones en caso de un incidente cibernético.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema potencial 7: Anomalías de la red (parte 1 & 2 de 5)

7.1 ¿Qué estoy buscando?

En ciertas jurisdicciones, una parte de la infraestructura electoral puede estar conectada de manera segura al internet. Es posible que observe **irregularidades o interrupciones** en la conexión de los sistemas electorales. Estas interrupciones podrían parecer una actividad repentina y excesiva en un sistema, o tiempos de respuesta inexplicables e inconsistentes de un sistema. Aunque usted no está allí para monitorear el tráfico de la red, podría observar una interacción frenética de un trabajador electoral con sus sistemas.

¿Por qué es esto importante?

Las irregularidades o interrupciones repentinas podrían indicar posibles ciberataques como un ataque de Denegación de Servicio Distribuido (DDoS), que es un ataque que busca abrumar y dejar inoperantes los sistemas electorales.

7.2 ¿ Qué estoy buscando?

En ciertas jurisdicciones, una parte de la infraestructura electoral puede estar conectada de manera segura al internet. Esté atento a cualquier **desconexión repentina o inexplicable** de un sistema electoral de internet o de la red aprobada (por ejemplo, una computadora portátil que de repente se desconecta).

¿ Por qué es esto importante?

Las desconexiones repentinas de los sistemas electorales podrían ser el resultado de un ciberataque que intenta aislar un sistema y interrumpir el proceso de votación.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema potencial 7: Anomalías de la red (parte 3 & 4 de 5)

7.3 ¿Qué estoy buscando?

En ciertas jurisdicciones, una parte de la infraestructura electoral puede estar conectada de manera segura a internet. Puede experimentar **retrasos inusuales en la velocidad de conexión.** Estos retrasos podrían ocurrir durante el funcionamiento normal de un sistema de votación o durante una fase especialmente crítica, como la tabulación o la transmisión de los totales de votos.

¿Por qué es esto importante?

La congestión o lentitud inexplicable de la red podría sugerir que un sistema está bajo algún tipo de ciberataque, como un intento de manipular su transmisión de datos.

7.4 ¿Qué estoy buscando?

En ciertas jurisdicciones, una parte de la infraestructura electoral puede estar conectada de manera segura al internet. Puede experimentar que **su actividad en línea sea redirigida** a un sitio web diferente o inesperado o a una ventana emergente. El sitio web al que es dirigido podría verse ligeramente 'extraño', con gráficos inusuales o pixelados, o una ventana emergente podría solicitarle que inicie sesión nuevamente de repente.

¿Por qué es esto importante?

Un sistema que es redirigido a un sitio web desconocido o inusual, o a una ventana que requiere volver a ingresar la identificación de inicio de sesión y la contraseña, podría ser una señal de un intento malicioso de secuestro para desviar o interceptar datos críticos de votación.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema potencial 7: Anomalías de la red (parte 5 de 5)

7.5 ¿Qué estoy buscando?

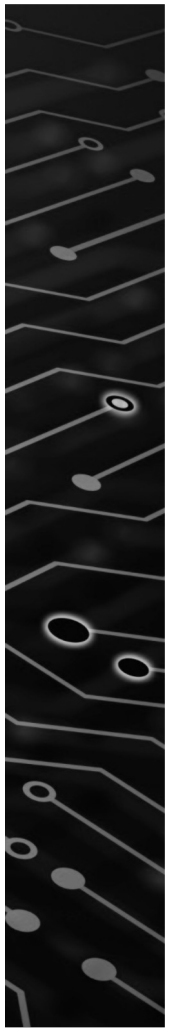
En ciertas jurisdicciones, una parte de la infraestructura electoral puede estar conectada de manera segura a internet. Puede experimentar una **transferencia de datos inusualmente rápida** o una transferencia de datos que de repente desaparece.

¿Por qué es esto importante?

El comportamiento inusual de los datos puede ser un signo de robo o manipulación maliciosa de los datos de votación, lo cual podría socavar la integridad o la equidad de una elección.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema potencial 8: Fuga o Violación de Datos Sensibles



¿Qué estoy buscando?

Tome muy en serio cualquier **sospecha de fuga** o violación de datos. Esto podría ser el envío involuntario de un correo electrónico con datos sensibles, el envío involuntario de un archivo adjunto con datos de votantes o de votación, la carga de datos sensibles a un sitio web incorrecto o la descarga no autorizada de datos en un dispositivo de almacenamiento externo (como una memoria USB). Una fuga de datos también podría parecerse a un conjunto de datos que normalmente tiene acceso y que de repente se vuelve inaccesible o desaparece.

Además, preste especial atención a cualquier **acceso sospechoso a datos,** ya sea en forma física o digital, como el manejo inadecuado de boletas en papel, el acceso digital al software electoral fuera del protocolo (ver también Problema Potencial 1) o señales de acceso remoto a un sistema electoral (un cursor moviéndose en la pantalla o palabras siendo escritas cuando el usuario no está realizando ninguna de estas actividades).

¿Por qué es esto importante?

Con acceso a los datos de votación o al software y sistemas que los procesan, los conjuntos de datos podrían ser 'envenenados', los modelos analíticos utilizados para contar los votos podrían ser manipulados o los datos podrían ser extraídos por completo. Cualquier acceso malicioso o fuga de información de los votantes también podría comprometer la privacidad o seguridad de los votantes.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema potencial 9: Falta de Registros del Sistema

¿Qué estoy buscando?

Cada sistema técnico escribe un rastro digital, un registro, de todo lo que 'hace', desde: encenderse y apagarse, hasta el acceso legítimo por parte de un funcionario electoral o proveedor, las operaciones del propio software y la recopilación y movimiento de datos (votos, tabulación de votos).

Cada máquina debe tener **habilitado el registro de todas las actividades técnicas.** Los registros del sistema deben preservarse de acuerdo con la ley estatal. Los detalles de la preservación deben incluir protocolos para la cadena de custodia, ubicación del almacenamiento de los registros, parámetros para el almacenamiento (cifrado de datos, seguridad física de las áreas de almacenamiento) y la duración requerida del almacenamiento.

¿Por qué es esto importante?

Los registros mostrarán actividades autorizadas **y** no autorizadas, y pueden ser inspeccionados posteriormente si surge alguna impugnación o si se sospecha de un problema. La ausencia de registros o interrupciones en la actividad de registro son una señal de alerta y pueden hacer que los incidentes de seguridad pasen desapercibidos o no puedan ser investigados.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema potencial 10: No Hay un Plan de Respaldo para una Interrupción o Incidente

¿Qué estoy buscando?

Confirme con todos los trabajadores electorales el **'Plan B' o plan de contingencia** en caso de que haya una interrupción del sistema durante el Día de las Elecciones.

Los trabajadores electorales deben tener un proceso documentado que seguirán, del cual también se beneficiarán si reciben capacitación. Los procesos de respaldo (como el uso de boletas en papel si los sistemas fallan) deben ser bien comprendidos por los trabajadores electorales, y los suministros necesarios para llevar a cabo el plan de contingencia deben estar fácilmente disponibles.

From a a best practices perspective, a Plan B could include:

- Una copia segura en papel de la Lista Oficial de Votantes Registrados
- La capacidad de emitir boletas en papel a los votantes elegibles en el sitio (si el sitio generalmente está totalmente impulsado por tecnología).
- Un mecanismo seguro para recolectar, tabular y almacenar esas boletas en papel una vez completadas por cada votante.

¿Por qué es esto importante?

Una interrupción prolongada de los sistemas informáticos el Día de las Elecciones sin un Plan de Respaldo adecuado podría negar a los ciudadanos su derecho a votar, socavando la integridad y la equidad de la elección.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema Potencial 11: Intentos de Phishing en el Personal Electoral

¿Qué estoy buscando?

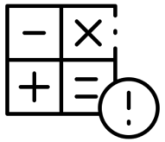
Esté alerta cuando usted o sus compañeros Trabajadores Electorales reciban **correos electrónicos o mensajes de texto sospechosos.** Phishes (correo electrónico) y Smishes (mensaje de texto) podrían estar siendo enviados a su correo electrónico o teléfono personal, o incluso a las capacidades de mensajería en un sistema electoral (por ejemplo, una estación de votación electrónica o una computadora portátil), si ese sistema tiene capacidad inalámbrica habilitada (ver también Problema Potencial 7.1).

¿Por qué es esto importante?

El phishing y el smishing son herramientas que los actores malintencionados utilizan para engañar fácilmente a las personas con mensajes tentadores y aparentemente reales, lo que puede llevar a que una persona ingrese sus credenciales de inicio de sesión en un sitio web falso o envíe información de votación sensible a un sitio malicioso.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema potencial 12: Discrepancias de Votación e Irregularidades en el Conteo de Boletas respecto al Conteo de Votantes



¿Qué estoy buscando?

Sea especialmente sensible a cualquier **votante que afirme que su voto no se está registrando con precisión.** Por ejemplo, un votante podría quejarse de que la selección que hizo en su sesión de máquina de votación *no se refleja con precisión* en la impresión en papel (su boleta) que se supone debe validar antes de insertarla en la máquina de votación final.

Esté también atento a cualquier **irregularidad entre los recuentos electrónicos de votos** y las copias de seguridad en papel al final del día y/o cualquier otro conteo del número de votantes del día. Cualquier discrepancia en el número podría indicar un problema a nivel del sistema con los datos o un mal funcionamiento del sistema. Al final del día de votación, el número de personas que ingresaron para votar debería coincidir exactamente con el número de boletas y recuentos en los sistemas en esa ubicación.

¿Por qué es esto importante?

El software electoral podría tener un problema de código, ya sea involuntario o malintencionado, que interprete digitalmente de manera incorrecta lo que un votante ingresa en la pantalla del sistema al registro del voto. Este problema podría interferir con la integridad de la elección.

Cualquier discrepancia entre el número de personas físicas que ingresaron y el conteo final de votos en las máquinas podría indicar manipulación, ya sea con votos individuales o con todos los datos de votación de ese día.

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

Problema potencial 13: Amenazas Internas

¿Qué estoy buscando?

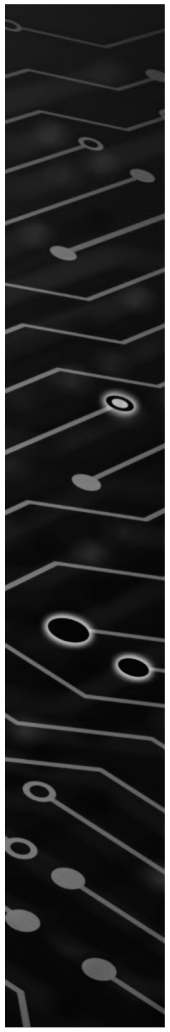
Esté atento a cualquier **comportamiento sospechoso de personas autorizadas** en y alrededor de los sistemas de votación, incluidos proveedores de TI, Trabajadores Electorales u otros Proveedores Externos... incluso el personal de mantenimiento del edificio. El comportamiento sospechoso podría incluir cosas que hemos cubierto en esta Guía, así como:

- Una persona que intenta anular los protocolos de seguridad de los sistemas
- Acceso en momentos inusuales a un sistema o sala donde los sistemas están almacenados de forma segura
- Insistencia en iniciar sesión en un sistema al que su rol normalmente no tiene acceso
- Desalentar o bloquear la actividad legal de Observadores Electorales o Supervisores de Elecciones.

¿Por qué es esto importante?

Incluso las personas 'verificadas' pueden usar su influencia y posición para realizar actividades fuera del alcance de su rol o que socaven los buenos protocolos de ciberseguridad. A través de su comportamiento, las personas de confianza pueden afectar la integridad de la elección.

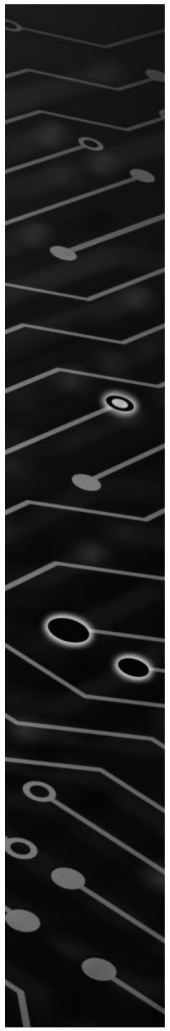
©2024 Institute for Cyber Civics, LLC. All Rights Reserved



Sobre El Instituto

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

El Instituto para Ciber Civica



Nuestra Pasión
Llevando lo mejor del conocimiento, habilidades y prácticas de ciberseguridad de las empresas Fortune 500 a la vida cívica cotidiana y a las interacciones de las personas con el universo digital.

Nuestra Misión
Somos una organización sin fines de lucro con la Misión de avanzar en la seguridad, protección, privacidad e integridad digital de las experiencias que los ciudadanos tienen al usar tecnología, IA y datos digitales en su vida cotidiana. Para apoyar los derechos y responsabilidades de los ciudadanos en el universo digital, el Instituto desarrolla y ofrece educación en ciberseguridad de vanguardia, investigación y defensa basada en las mejores prácticas de ciberseguridad de las empresas Fortune 500, adaptadas a los ciudadanos y sus experiencias digitales diarias.

Nuestras Alternativas
Nuestra prioridad inaugural es equipar a los funcionarios electorales estatales y del condado, observadores de casilla, líderes en ciberseguridad y proveedores de tecnología de sistemas de votación con el conocimiento y las herramientas necesarias para reducir los riesgos del proceso electoral ante las amenazas cibernéticas. Actualmente, nos estamos enfocando en las elecciones de EE. UU. de 2024, con el objetivo de eventualmente expandir nuestros esfuerzos para brindar orientación en elecciones en todas partes. Como parte de nuestra Misión, también abordaremos temas como prácticas cibernéticas seguras para jóvenes en redes sociales, uso efectivo de la ciberseguridad e IA para combatir el tráfico de personas, y consejos para la seguridad de la huella digital de los ciudadanos.

Visítanos en: https://InstituteforCyberCivics.org

©2024 Institute for Cyber Civics, LLC. All Rights Reserved

INSTITUTE FOR
CYBER CIVICS

¡Agradecemos sus comentarios sobre este manual!

Visítanos en: https://InstituteforCyberCivics.org

v1.1 October 2024

©2024 Institute for Cyber Civics, LLC. All Rights Reserved